

Amendment/Reply

Applicant: Norman C. Chou et al.

Serial No.: 10/057,159

Filed: January 24, 2002

Docket No.: 10011314-1/A610.258.101

Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE

JAN 04 2007**REMARKS**

This Amendment/Reply accompanies the Request for Continued Examination (RCE) 37 CFR 1.114 and is in reply to the Final Office Action mailed October 4, 2006.

The following remarks are made in response to the Final Office Action mailed October 4, 2006. Claims 1-34 were rejected. With this Amendment/Reply, claims 1, 3, 8, 12, 15-16, 22-23, 26-27, 33, and 34 have been amended. Claims 1-34 remain pending in the application and are presented for reconsideration and allowance.

Claim Rejections under 35 U.S.C. § 102

The Examiner rejected claims 1-34 under 35 U.S.C. § 102(a) as being anticipated by the InfiniBand Trade Association, (InfiniBand Architecture Specification Volume 1, Release 1.0.a, June 19, 2001 (the "InfiniBand reference").

The InfiniBand Architecture (IBA) is defined by the InfiniBand reference. In the IBA, an interconnect device typically includes a management port. Each sub-network (subnet) is managed by at least one Subnet Manager which performs its managing functions by communicating with the management port of an interconnect device using InfiniBand Subnet Management Packets (SMPs).

SMPs are used to initialize and configure switches and other interconnect devices, and are therefore considered to participate in privileged operations. As a result, a mechanism is provided to authorize subnet management operations by comparing authentication data included in a SMP with authentication data stored in a destination port. The authentication data includes a Management Key (e.g., the InfiniBand Management Key). The Management Key is associated with several attributes that may affect the authorization of subnet management operations. For example, these attributes may include a protection attribute (e.g., the InfiniBand M_KeyProtectBits) that identifies levels of protection required for specific subnet management operations and an expiration attribute (e.g., the InfiniBand M_KeyLeasePeriod) that allows the management key to "expire" if the management key is lost or contaminated. The expiration of the management key attribute is not permitted if the expiration attribute is set to zero. Accordingly, a problem may arise when the management key is lost or becomes contaminated while the expiration attribute is equal to zero.

Amendment/Reply

Applicant: Norman C. Chou et al.

Serial No.: 10/057,159

Filed: January 24, 2002

Docket No.: 10011314-1/A610.258.101

Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE

The Infiniband reference at 14.2.4.2 at p 657 specifically states "when the *PortInfo:MaxKeyLeasePeriod* is set to zero, the lease period shall never expire. Whether there is an out-of-band mechanism to reset data protected with a lease period of zero is outside the scope of the specification." Amended independent claims 1, 8, 12, 22, 23, 33, and 34 include limitations related to providing or facilitating mechanisms to reset authentication data having associated thereto an expiration attribute set to a value providing for indefinite duration of the authentication data. Embodiments of the present invention claimed in amended independent claims 1, 8, 12, 22, 23, 33, and 34 can accordingly provide or facilitate mechanisms to reset authentication data having associated thereto an expiration attribute set to a value providing for indefinite duration of the authentication data (e.g., protected with a lease period of zero) which is explicitly excluded from the Infiniband reference.

The specific limitations of the independent claims that allow a subnet manager or any other authorized entity to regain control over an interconnect device and reset authentication data having associated thereto an expiration attribute set to a value providing for indefinite duration of the authentication data (e.g., protected with a lease period of zero), and therefore explicitly not taught in the InfiniBand reference, are as follows.

Independent claim 1 includes a configuration switch configured to receive an operator command to reset authentication data having associated thereto an expiration attribute set to a value providing for indefinite duration of the authentication data, wherein the authentication data facilitates authorization of the management operations from an operator, and configured to generate a reset signal in response to the operator command, and a port of the interconnect device coupled to the configuration switch, the port configured to maintain the authentication data and to reset the authentication data upon receiving the reset signal from the configuration switch.

Independent claim 8 includes receiving a reset signal from a configuration switch at a decoder of a management port, the reset signal indicating that an operator requested a reset of an authentication data having associated thereto an expiration attribute set to a value providing for indefinite duration of the authentication data, wherein the authentication data facilitates authorization of the management operations, and resetting a copy of the authentication data, wherein the authentication data is stored in the decoder in response to the reset signal.

Amendment/Reply

Applicant: Norman C. Chou et al.

Serial No.: 10/057,159

Filed: January 24, 2002

Docket No.: 10011314-1/A610.258.101

Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE

Independent claims 12, 22, and 34 include limitations related to detecting that a reset is required of authentication data having associated thereto an expiration attribute set to a value providing for indefinite duration of the authentication data, wherein the authentication data resides in a management port of the interconnect device, informing an operator that the reset is required, refraining from sending subnet management packets (SMPs) to the management port upon detecting that the reset is required, receiving a message from the operator that indicates that the authentication data has been reset, and sending to the management port an update SMP with a request to set authentication data residing in each unit of the interconnect device to an update value.

Independent claim 23 includes an interconnect device to maintain authentication data in a plurality of units, the authentication data facilitating management operations associated with the interconnect device, a configuration switch coupled to the interconnect device, the configuration switch configured to reset authentication data having associated thereto an expiration attribute set to a value providing for indefinite duration of the authentication data, wherein the authentication data resides in a management port of the interconnect device, and a sub-network (subnet) manager coupled to the interconnect device, the subnet manager configured to detect that the reset of authentication data residing in the management port is required, to inform an operator that the authentication data has been reset, and to send to the management port an update data packet with a request to set the authentication data residing in each of the plurality of units of the interconnect device to an update value.

Independent claim 33 includes a decoder configured to reset, based on a reset signal received from a configuration switch, an authentication data having associated thereto an expiration attribute set to a value providing for indefinite duration of the authentication data, wherein the authentication data is stored in the decoder, and the decoder is configured to receive a management packet from the sub-network (subnet) manager with an update value for the authentication data residing in a plurality of units of an interconnect device, and a subnet management agent configured to receive the management packet from the decoder and to control the update of the authentication data residing in each of the plurality of units.

Therefore, independent claims 1, 8, 12, 22, 23, 33, and 34 all include limitations that are explicitly excluded from the InfiniBand reference. Therefore, these independent claims are not taught by the Infiniband reference.

JAN 04 2007

Amendment/Reply

Applicant: Norman C. Chou et al.

Serial No.: 10/057,159

Filed: January 24, 2002

Docket No.: 10011314-1/A610.258.101

Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE

Furthermore, dependent claims 2-7 further define patentably distinct independent claim 1; dependent claims 9-11 further define patentably distinct independent claim 8; dependent claims 13-21 further define patentably distinct independent claim 12; dependent claims 24-26 further define patentably distinct independent claim 22; and dependent claims 27-32 further define patentably distinct independent claim 23. Therefore, these dependent claims are believed to be allowable.

Therefore, Applicants respectfully request reconsideration and withdrawal of the 35 U.S.C. § 102(a) rejection to claims 1-34, and request allowance of these claims.

CONCLUSION

In view of the above, Applicant respectfully submits that pending claims 1-34 are in form for allowance and are not taught or suggested by the cited references. Therefore, reconsideration and withdrawal of the rejections and allowance of claims 1-34 is respectfully requested.

No fees are required under 37 C.F.R. 1.16(h)(i). However, if such fees are required, the Patent Office is hereby authorized to charge Deposit Account No. 50-3718.

The Examiner is invited to contact the Applicant's representative at the below-listed telephone numbers to facilitate prosecution of this application.

Amendment/Reply

Applicant: Norman C. Chou et al.

Serial No.: 10/057,159

Filed: January 24, 2002

Docket No.: 10011314-1/A610.258.101

Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE

Any inquiry regarding this Amendment/Reply should be directed to either Patrick G. Billig at Telephone No. (612) 573-2003, Facsimile No. (612) 573-2005 or John R. Pessetto at Telephone No. (303) 298-9888, Facsimile No. (303) 297-2266. In addition, all correspondence should continue to be directed to the following address:

AVAGO TECHNOLOGIES, LTD.
P.O. Box 1920
Denver, Colorado 80201-1920

Respectfully submitted,

Norman Chou et al.,

By their attorneys,

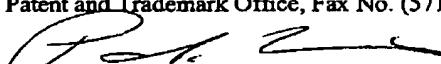
DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2003
Facsimile: (612) 573-2005

Date: 1-4-07

PGB:cmj:dmw


Patrick G. Billig
Reg. No. 38,080

CERTIFICATE UNDER 37 C.F.R. 1.8: The undersigned hereby certifies that this paper or papers, as described herein, are being facsimile transmitted to the United States Patent and Trademark Office, Fax No. (571) 273-8300 on this 4 day of January, 2007.

By 
Name: Patrick G. Billig